



## Security Framework - A Case Study of a Higher Education Institution

Wail Mohammad Dar

Department of Computer Science,

School of Technology

Islamic University of Science and Technology

Awantipora. Pulwama J&K- India

---

**Abstract**— Security consideration is a very important issue in every organization today. It is the main concern today to have a very secure information system in place so that hackers from outside and the websites hosted on the servers cannot be attacked or disfigured or the contents cannot be changed by some mischievous elements causing harm to the organization. It is therefore very important that Network / server administrators are aware about the attacks and malicious or unwanted computing agents who always try to breach the security and attempt to steal important information from the servers. Therefore the security frame work or the procedures that are essential and necessary at all levels in the organization be implemented so that unauthorized access is strictly restricted. In this regard every organization follows a security policy and security framework in order to achieve its objectives for its entirety. With reference to the Higher Education Institutions in the J&K State, a leading State university namely Kashmir University was taken as a case study for this research.

**Keywords** — Kashmir University, Hacker, Security policy, unauthorized access, unwanted computing agent.

---

### I. INFORMATION SECURITY POLICY

This policy provides a framework for the management of information security throughout the University. It applies to:

- All those with access to University information systems, including staff, students, visitors and contractors.
- Any systems attached to the University computer or telephone networks and any systems supplied by the University;
- All information (data) processed by the University pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from the University and any University information (data) held on systems external to the University's network;
- All external parties that provide services to the University in respect of information processing facilities and business activities.
- Principal information assets including the physical locations from which the University operates.

In order to achieve those above mentioned objectives following procedure is followed here in University of Kashmir.

### II. USER PASSWORD MANAGEMENT

#### A. Password Complexity Requirements

The University Of Kashmir must enforce password complexity requirements for all accounts on all systems.

The University Of Kashmir password complexity requirement must include at a minimum password length of seven characters, consisting of at least two of the following character sets:

- Lowercase characters (a-z)
- Uppercase characters (A-Z)
- Digits (0-9)
- Punctuation and special characters.

To encourage strong passwords the University of Kashmir to consider the use of password setting/changing routines that provide feedback to the user as to the password's strength. To encourage strong passwords the University of Kashmir to consider a shorter password expiry timeframe (i.e. 30 days) for weaker passwords and a longer expiry timeframe (ie 120 days) for strong passwords – 60 day expiry being the norm for medium strength passwords. Where systems cannot be

configured to enforce complexity requirements, The University of Kashmir must check passwords for compliance with their password selection and complexity requirements.

#### ***B. Password Change and Reuse***

The University Of Kashmir must prevent the following activities during password change and reset:

Password reuse across multiple accounts. Password reuse within 5 password changes. Use of sequential passwords Use of predictable passwords.

The University Of Kashmir must ensure that passwords for all accounts on all systems and devices are changed at least every 180 days. The University Of Kashmir must prevent system users from changing their password more than once a day.

#### ***C. Password Reset Procedures***

The University Of Kashmir must ensure that system users provide sufficient evidence to verify their identity when requesting a password reset.

### **III. SUSPENSION OF ACCESS**

The University Of Kashmir must suspend user accounts in the following circumstances.

- Three failed login attempts.
- Suspected malicious activity.
- Suspected inappropriate behaviour.

In the case of failed logins, accounts must only be automatically unlocked after 10 minutes.

In the case of malicious or inappropriate behaviour, suspended accounts must be unlocked by an authorized systems administrator.

### **IV. CHANGING ROLES**

The University Of Kashmir must ensure that upon changing role within the organization, any user accounts, access permissions or group memberships granted to the user are reviewed and removed where no longer required. This must be applied to employees, contractors and sub-contractors.

This must be applied to temporary and permanent role changes.

Where a user had access to systems or devices that do not use centralized authentication, all devices must checked and relevant accounts removed.

Any shared passwords known by or accessed by the user must be changed immediately.

### **V. LEAVING THE ORGANIZATION**

The University of Kashmir must ensure that upon leaving the organization, all accounts for a user are disabled. This must be applied to employees, contractors and sub-contractors. Any shared passwords known by or accessed by the user must be changed immediately.

#### ***A. Inactive Accounts***

The University of Kashmir must conduct monthly reviews of all user and system accounts and identify all accounts that have been inactive for 180 days or more.

#### ***B. Network Access Control***

To prevent unauthorized access to the University of Kashmir networked services - access to both internal and external networked services must be controlled.

#### ***C. Network Connection Control***

Direct public access must be restricted between external networks and any system component that stores restricted data. Internal network access must be restricted depending on the user and device credentials, with access granted based on user access permissions and the device's security profile.

#### ***D. Network Routing Control***

Inbound and outbound traffic must be restricted to that which is necessary for the restricted data environment only - with all other inbound and outbound traffic not being allowed.

### **VI. OPERATING SYSTEM ACCESS CONTROL**

To prevent unauthorized access to the University of Kashmir operating systems, security facilities must be used to restrict access to operating systems to authorized users.

## **VII. SYSTEMS CONFIGURATION AND MONITORING**

### **A. Authentication Methods:**

The University of Kashmir must monitor developments in authentication technologies to ensure that this standard and any associated procedures are kept up to date with current security good practice.

### **B. Device Configuration**

Vendor-supplied default passwords must be changed prior to installing a system on the University of Kashmir's network. Where available, all system components must be configured to use centralized authentication systems.

### **C. Use of Personal Devices**

Device maintenance and security for personal mobile computing and communication devices (including but not limited to laptops, tablets and mobile phones) remains the responsibility of the asset owner. The University of Kashmir must inform all users of personal devices of their security obligations concerning mobile computing devices. Personal devices must only connect to The University of Kashmir networks designated for such usage. These include mobile device and guest networks only. The University of Kashmir must prevent personal and unknown mobile computing devices from connecting to all other University of Kashmir systems with restricted data.

### **D. Use of University Devices**

Personal firewalls and anti-virus must be installed on all of the University of Kashmir issued laptop computers and mobile computing devices. All of the University of Kashmir mobile computing devices must be registered as per the University of Kashmir mobile device management policy. The user will be responsible for the secure storage and management of mobile computing device.

The University of Kashmir must conduct an audit of all of the University of Kashmir provided mobile computing devices on an annual basis. This audit must:

Physically verify the device and its condition, Identify any damage or modifications since issue .Verify device registration details and Verify the allocated user remains unchanged.

The University of Kashmir issued mobile computing devices must be returned upon leaving the organization (including all issued peripherals and storage media).

### **E. Network Usage**

When connecting with a mobile device on campus, University of Kashmir staff and students must only connect to designated networks for mobile devices (including Wi fi and tethering).

The University of Kashmir must ensure that personal or unknown devices are prevented from connecting to the secure internal University of Kashmir networks.

## **VIII. Remote Access Governance and Management Authorization**

*Remote access authorizations should be reviewed annually.*

### **A. Logging and Monitoring**

All remote access activity must be logged and monitored in line with the University of Kashmir Vulnerability Management standard.

### **B. Configuration and Operation**

#### *1) Authentication*

Strong authentication must be used for remote access to the network by staff and authorised third parties. Where exceptions to this item are required (such as guest and mobile wireless networks), these networks must be segregated from core University of Kashmir data storage systems and networks. Remote access must not be permitted using system administration accounts, or accounts with system administration privileges. Device and Systems Configuration, the University of Kashmir strongly encourages that remote devices employ anti-virus and firewall software.

## **IX. Formation Systems Acquisition, Development and Maintenance**

### **A. Systems Security Requirements**

The design and implementation of the University of Kashmir systems can be crucial for information security. Security requirements must therefore be identified and agreed prior to the development and/or implementation of the University of Kashmir systems.

### **B. Development of Operational Standards**

The University of Kashmir must develop daily operational security procedures that are consistent with the requirements of this Information Security standard. All information systems must be managed in accordance with industry best practice.

Documented Standard Operating Procedures must be prepared for all those system activities associated with information processing and communication facilities. Therefore the following must be considered:

- System start-up and close-down;
- Backups;
- Equipment maintenance;
- Media handling;
- System version;
- Application versions;
- Secure area working;
- Health and safety.

### **C. Responsibility and Accountability**

Departmental IT Managers are responsible for ensuring the development, maintenance, updating and implementation of any Standard Operating Procedures (SOPs).

### **D. Control and Definition of Process**

The University of Kashmir change control procedures must be documented and peer reviewed in order to protect the integrity, availability and confidentiality of the University of Kashmir's information systems. Formal management responsibilities and procedures must be in place to ensure satisfactory control of all changes to equipment, software or procedures. The Manager, IT Infrastructure must approve all changes that impact the security of The University of Kashmir information and systems.

## **X. CONTROL ITEMS**

The following change control management control items must be considered:

- Identification and recording of all significant changes;
- Planning and testing of changes;
- Assessment of the potential information security impacts of such changes;
- Formal approval procedure for proposed changes;
- Communication of change details to all relevant persons including third parties; and
- Rollback procedures (including processes and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events).

Any change procedure must also include:

- Maintaining a record of agreed authorisation levels;
- Ensuring changes are submitted by authorised users only;
- Reviewing relevant controls and integrity procedures to ensure they will not be compromised by the changes;
- Identifying all software, information, database entities, and hardware that require amendment;
- Obtaining formal approval for detailed proposals before work commences;
- Ensuring authorised users accept changes prior to implementation;
- Ensuring that the system documentation set is updated on the completion of each change;

## **XI. AUDIT AND LOGGING**

When changes are made, an audit log containing all relevant information must be retained for a minimum of 5 years.

### **A. Test Data**

Live production data is not to be used for testing or development. Development and test databases derived from production data must have the same level of security controls as the production databases.

## **XII. MONITORING AND REVIEW OF THIRD PARTY SERVICE**

### **A. Right to Audit**

The University of Kashmir must ensure that the 'right to audit' is included in every commercial service agreement. The 'right to audit' must extend to a minimum of the following activities:

- Penetration Testing;
- Vulnerability Assessment;
- Configuration Review;
- Information Security Audit; and
- Physical Review (Premises, Data centres).

### **XIII. SERVICE LEVELS AND INFORMATION SECURITY**

The University of Kashmir must review the service levels provided by external providers on at least annual basis to ensure that all obligations have been met. The University of Kashmir must include information security objectives in external provider service level reviews.

#### **A. Use of Cryptographic Controls for wireless environments:**

- Enable Wi-Fi Protected Access technology for encryption and authentication when WPA2-capable and updated when possible;
- A complex password should be used that includes capitals and lower case letters, numbers and characters with the minimum length of 8 characters; WIFI passwords where used must be changed every annually;
- Change wireless vendor defaults (including - but not limited to - default SSID, passwords, and SNMP community strings)

#### **B. Disk and Database Encryption**

- If disk (rather than file- or column-level database) encryption is used, logical access must be managed independently of native operating system access control.
- All data classified CONFIDENTIAL and above must be encrypted in storage and in transfer (SSL); and All data classified CONFIDENTIAL and above must be encrypted in physical transit. Decryption keys must not be tied to user accounts.

### **XIV. CRYPTOGRAPHIC KEY MANAGEMENT**

#### **A. Key Storage**

The University of Kashmir must provide details of how the key(s) will be electronically and physically stored and transferred to different sites.

- Keys must not be stored on the same media as the encrypted data; and
- All cryptographic keys should be stored in an encrypted state.

The University of Kashmir must reserve the right to amend, terminate or otherwise renegotiate all agreements with external parties based on reviews.

### **XV. Vulnerability Management: Attack Surface Awareness**

The University of Kashmir must maintain a record of system components in use across The University of Kashmir systems. This record should include:

- Operating Systems (including versions)
- Software packages and installed components
- Libraries, development frameworks and application components

The University of Kashmir must use this record to focus vulnerability awareness activities including:

- Patching and system updates
- Systems configuration and hardening
- Technology upgrades
- Installation of defensive security measures
- Systems monitoring
- Education and Training

#### **A. Dissemination of Vulnerability Information**

The University of Kashmir must assign responsibility for the dissemination of vulnerability information to all relevant technical area and systems risk owners.

#### **B. Systems Development and Vulnerability Assessment**

The University of Kashmir must establish a process to identify newly discovered security vulnerabilities, and standards must be updated to address these. The University of Kashmir must ensure all web-facing applications are protected against known attacks by running internal and external network vulnerability scans: prior to initial system use every 2 months, after any significant change in the network.

#### **C. Configuration Standards and Processes**

Configuration standards must be developed for all system components which must address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. All unnecessary and insecure services, protocols and

functionality must be disabled (e.g.: scripts, drivers, features, subsystems, file systems, and unnecessary web servers). System security parameters must be configured to prevent misuse.

#### ***D. Transfer of Executable Files***

The University of Kashmir must ensure that users are prevented from sending and receiving executable or malicious files using The University of Kashmir email system.

#### ***E. Anti-Virus***

Anti-virus software must be deployed on all WIN and MAC OS systems. The University of Kashmir must ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software - including spyware and adware. All anti-virus mechanisms must remain current, actively running, and capable of generating assessment logs. The University of Kashmir must ensure that all anti-virus applications are updated daily.

#### ***F. Control of Technical Vulnerabilities***

Configuration standards must be developed for all system components which must address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. All unnecessary and insecure services, protocols and functionality must be disabled (e.g.: scripts, drivers, features, subsystems, file systems, and unnecessary web servers). System security parameters must be configured to prevent misuse. The University of Kashmir must establish a process to identify newly discovered security vulnerabilities, and standards must be updated to address these. Software applications must be based on industry best practices and incorporate information security throughout the software development life cycle.

#### ***G. Reporting Information Security Events and Weaknesses***

To ensure Information security events and weaknesses associated with the University of Kashmir's data and systems are communicated in a manner allowing timely corrective action to be taken - formal event reporting and escalation standards must be in place.

#### ***H. Identification of Critical Systems***

The University of Kashmir must identify all systems within the organization that are critical to the continuation of core business functions.

All critical systems must be documented as the 'Critical Systems List'.

The 'Critical Systems List' must include at a minimum:

- Name
- Function
- System Owner
- Physical Location
- Dependencies
- Date Last Updated

### **XVI. RISK ASSESSMENT AND PRIORITIZATION**

The identification of possible events must be followed by a formal risk assessment to determine the probability and impact of such interruptions - in terms of time, damage scale and recovery period. Business continuity risk assessments must be carried out with full involvement from the owners of The University of Kashmir's business resources and processes. Any risk assessment must consider all business processes and not be limited to The University Kashmir's information processing facilities only - but must include the results specific to information security. Any risk assessment must identify, quantify, and prioritize risks against criteria and objectives relevant to The University of Kashmir- including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

### **XVII. INDUSTRY STANDARDS**

The University Of Kashmir must comply with ISO 27001/27002

Audit logs recording user activities, exceptions and security events should be produced and for an agreed period to assist in future investigations and access control monitoring. NIST SP 800-53 includes a list of 12 relevant event types and 3 categories of services:

Management, Operational and Technical

#### ***A. Management Services***

Security Program, Security policy, Risk Management, Security Architecture Certification and Accreditation, and Security Evaluation of IT products.

**B. Operational Services**

Contingency Planning, incident handling, testing and training

**C. Technical Services**

Firewalls, Intrusion Detection/Prevention and Public Key infrastructure.

**APPENDIX A  
SECURITY RESPONSIBILITIES MATRIX FOR UNIVERSITY OF KASHMIR**

		<b>Controls</b>	<b>IT</b>	<b>Division\Faculty</b>
1	Security Policy	Document	S	
		Ownership		
		Review	P	
2	The Organization of Security	Information Security Co-ordination	P	S
		Information Security activities	P	S
		On-going Information Security Activities	P	S
		Information Security Risk Management	P	
		Authorisation Process for Information Processing Systems	P	S
		Contractual Requirements	P	S
		Incidents and Contact with External Authorities	P	
		Review of Information Security	P	S
		Service Delivery (external parties)	P	S
3	Asset Management	Asset Inventory	P	S
		Securing the Asset Lifecycle	P	S
		Acceptable Use of Assets	S	S
		Information labelling and Classification	P	S
4	Human Resources Security	Roles and Responsibilities		S(HR)
		Background Screening and Checking		P(HR)
		Terms and Conditions of Employment		P(HR)
		Management Responsibilities		
		Information Security Awareness, Education, and Training	P	S
		Termination Responsibilities	S	P
	Removal of Access Rights	P	S	

		<b>Controls</b>	<b>IT</b>	<b>Division\Faculty</b>
5	Physical and Environmental Security	Physical Security Perimeters	P	S (FMD)
		Physical Entry Controls	P	S (FMD)
		Physical Security Obligations and Incidents	P	S (FMD)
		Secure Systems Configuration and Defence	P	S
		Equipment Maintenance	P	P
		Security of Equipment Off-Premises	P	P
6	Communications and Operations Management	Documented Operating Standards	P	S

Change Control Management	P	S
Separation of Development, Test and Production Facilities	P	P
Monitoring and Review of Third Party Services	P	P
Capacity Management	P	P
System Acceptance (Third Party)	P	
Controls against Malicious Code	P	P
Information Backups	P	P
Network Controls	P	S
Management of Media	P	S
Media Handling	P	P
Disposal of Media	P	P
Information Handling Standards	P	P
Exchange Agreements	P	P
Physical Media in Transit	P	P
Electronic Messaging	P	P
Assessment Trails	P	S
Monitoring System Use	P	S
Protection of Log Information	P	S
	P	S

**Legend:**

**P = Primary Responsibility**

**S= Secondary Responsibility**

**XVIII. Conclusion**

The case study in this article thus demonstrated that the use of the policy framework for any organisation is a basic road map for planning , implementing and securing the information content so that attackers/hackers and other unwanted computing agents etc are identified well in time so that information in an organisation can be secured in all means. Otherwise measures, policies and mechanisms demonstrated above generally fail if they are not accepted or implemented properly.

**REFERENCES**

1. Avolio, F. (2000). "Best Practices in Network Security." Network Computing 11(5):
2. Clark-Dickson, P. (2001). "Alarmed and Dangerous." e-Access March 2001
- Conolly, P. (2000). "Security Starts from Within." InfoWorld 22(28): 39-40.
3. Hartley, B. (1998). "Ensure the Security of Your Corporate Systems (Developing a Security Policy)." E-Business Advisor 16(6): 30-32.
4. Hinde, S. (1998). "Recent Security Surveys." Computers and Security 17(3): 207-210.
5. NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.
7. Janice C. S & Burke T. W (2008). A Framework for Information Security Management based on Guiding Standards: A United States Perspective, volume 5.
8. Security Framework. Putting Basic Security Principles To Work. Retrieved December 10, 2008.
9. William S. (December 2007). Standards for Information Security Management. The Internet protocol Journal, volume 10 No. 4. From [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_10-4/104\\_standards.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_standards.html).
10. Abdulkader Alfantookh. An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls. Computer Sciences, King Saud University. 2009.
11. Chris Potter & Andrew Beard. Information Security Breaches Survey 2010. Price Water House Coopers. Earl's Court, London.2010.
12. Heru Susanto, Mohammad Nabil Almunawar & Yong Chee Tuan.ISoIFramework: as a Tool for Measurement and Refinement of
13. Information Security Management Standard. On review paper. 2012b.